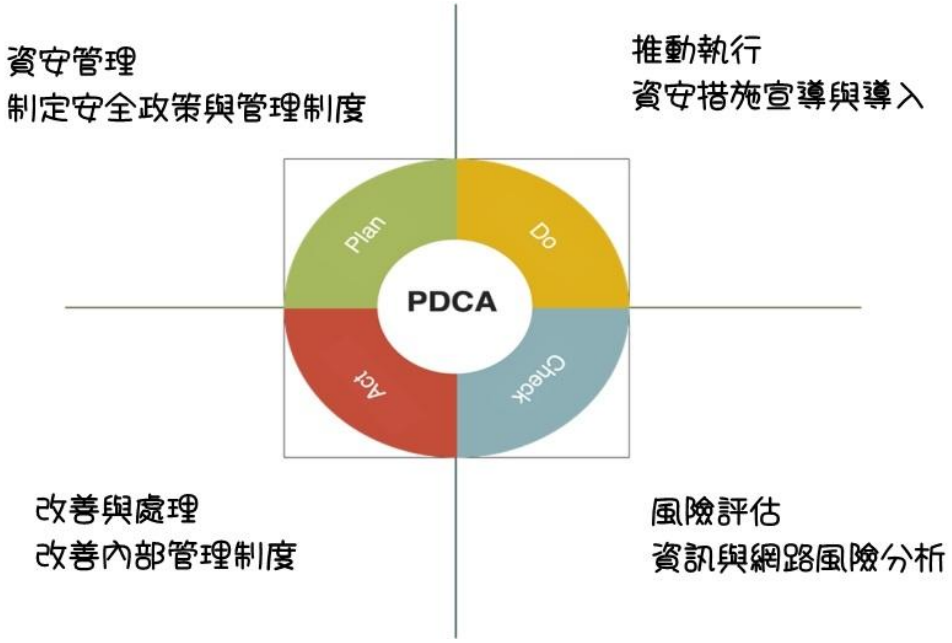
資訊安全風險管理架構

1.組織

本公司資訊安全之權責單位為資訊部，負責規劃、執行及推動資訊安全管理事 項，並推動資訊安全意識及落實管理。為強化本公司之資訊安全管理、確保資料、系統及網路安全，設立資訊安全主管與資安人員。

公司在資訊安全管理方面，有建置網路與系統的安全系統，訂有「電腦資訊安全政策」並每年一次檢討向總經理報告，其強化資訊安全，落實電腦資訊使用管理，維護電腦資源有效運用，以期整體資訊業務順利進行。

組織運作模式採 PDCA（Plan-Do-Check-Act）循環式管理，確保可靠度目標之達成且持續改善。



2. 資訊安全風險管理機制

進行機房設備、網路安全、病毒防護與電子郵件管理、資訊系統存取與維運、人員教育訓練等安全管理措施，強化公司資安防護能量。

- 主機室門禁管理辦法
- 網路開放相關規定事宜
- 資料庫備份辦法
- 主要系統還原測試演練
- 電子郵件管理與使用規範
- 資訊系統管理辦法
- 資訊安全通報事件處理流程
- 防毒軟體管理
- 人員教育訓練

3. 資訊安全政策

建立安全及可信賴之電腦化作業環境，確保本公司資料、系統、設備及網路安全，以保障公司利益及各單位資訊系統之永續運作。

(1) 總則
(2) 人員安全管理及教育訓練
(3) 電腦系統安全管理
(4) 網路安全管理
(5) 系統存取控制
(6) 系統發展與維護安全管理
(7) 資訊資產之分類與管理
(8) 業務永續運作之規劃

4. 資訊與網路風險分析

資產名稱	風險事件		可控制的措施或處置
	弱點	衍生之威脅	
伺服器主機	作業系統漏洞	導致系統被入侵	不定期進行作業系統漏洞修補測試或網路之管控
	硬體設備損毀	主機無法運作	主機虛擬化或另備實體主機備援
	軟體資料無備份	資料遺失損毀	定期進行檔案異地備援
	帳號密碼控管	資料外流或竄改	帳號密碼定期變更及複雜度
	不可避之天然災害	主機損毀	虛擬化主機資料異地備份保存
個人電腦	作業系統漏洞	導致系統被入侵	不定期進行作業系統漏洞修補或網路之管控
	電腦病毒	電腦無法運作	個人防毒軟體安裝及定期更新
網路設備	網路協定漏洞	網路無法使用	網路協定之管控或主機韌體更新
	不可避之天然災害	設備無法運作	另備相關網路設備備援
員工	資安觀念不足	電腦中毒或資料被竊	不定期資安觀令宣導及教育

5. 資訊安全通報事件處理

資訊安全事件包括：系統被入侵、對外攻擊、針對性攻擊、散播惡意程式、中繼站、電子郵件攻擊、垃圾郵件、命令或控制伺服器、殭屍病毒、惡意網頁、惡意留言、網頁置換、釣魚網頁、個資外洩以及網路中斷等。

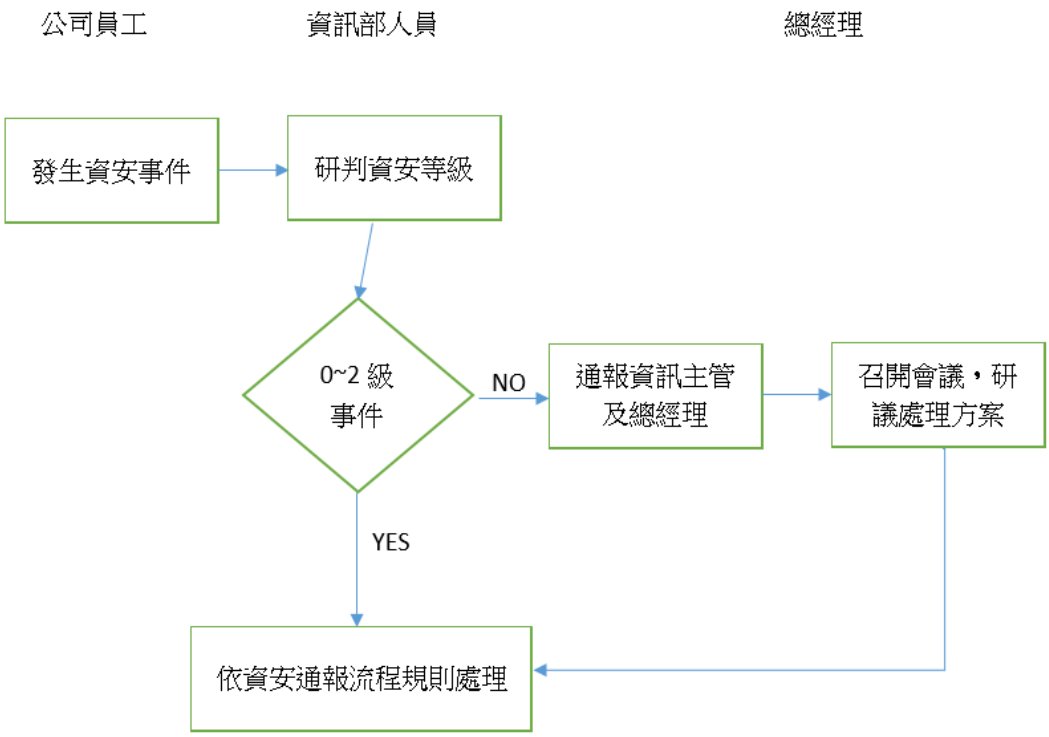
5-1 資訊安全事件等級

本公司資訊安全事件等級，由輕微至嚴重區分成 4 個等級。

等級	說　　明
0 級	(1) 其他單位所告知發生未確定之資安事件 (2) 檢舉信箱通告之資安事件
1 級	(1)非核心業務資料遭洩漏 (2)非核心業務系統或資料遭竄改。 (3)非核心業務運作遭影響或短暫停頓。
2 級	(1)屬密級或敏感之核心業務資料遭洩漏。 (2)核心業務系統或資料遭輕微竄改。 (3)核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。
3 級	(1)密級或敏感公務資料遭洩漏。 (2)核心業務系統或資料遭嚴重竄改。 (3)核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

- 任何人於公司內發現異常情況或疑似資安事件，應立即向資訊部通報，資訊人員儘速處理並研判事件等級。
- 資訊人員當發生研判事件等級 3（含）以上之事件，應立即通報資訊主管，由資訊主管儘快召集會議研商處理的方式。
- 資安通報依情報來源分為「告知通報」與「自行通報」，若收到「告知報」事件通知，由資安業務承辦人留下記錄，完成通報及應變作業。
- 資安事件須於發生後 1 小時內進行通報，0、1、2 級事件於事件發生後 72 小時內處理完成並結案(包括通報與應變)，3 級事件於事件發生後 36 小時內完成並結案。

5-2 資安事件通報程序



6. 實施資安的影響與因應措施

公司對資訊系統的投資不遺餘力，主要能提升管理與競爭力，相對地就越來越依賴資訊系統，所以強化異地備援與資料備份機制是不可或缺的，就是要讓系統服務不中斷。但近來資安事件頻繁，服務中斷不再限於天災與人為疏失，分析其主要來自外部攻擊為大宗，其次是內部員工欠缺資安意識與疏失造成，因此會加強員工的教育訓練與系統漏洞的防堵，最重要的是不定時的演練備援回復機制，以防資安事件造成公司的損失。